UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Incidenti informatici nella Pubblica Amministrazione: gestione ed obblighi di notifica tra GDPR e NIS2

Amalia Braggion

3 ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Contesto

Digitalizzazione rapida della PA: un processo che ha portato benefici in termini di efficienza e trasparenza ma che tuttavia, non è stato adeguatamente accompagnato da un potenziamento della **gestione del rischio cyber**

Rapporto Clusit 2025

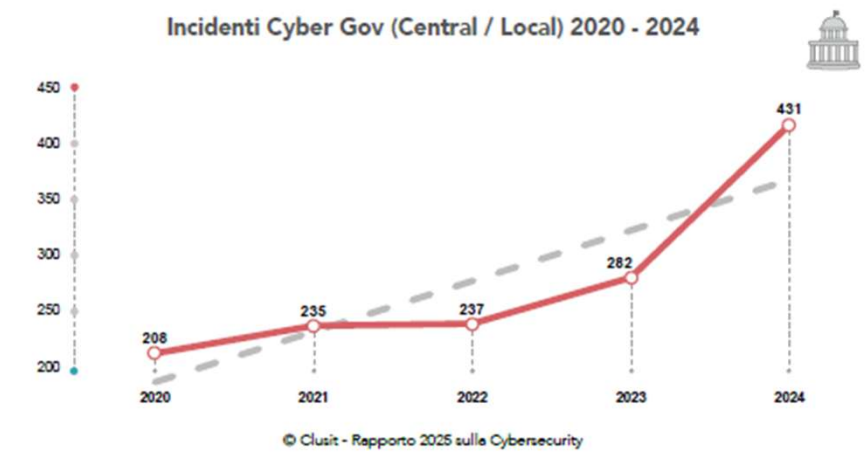

Fig. 19 - Incidenti al settore Gov (Central / Local) nel periodo 2020-2024

Analisi degli incidenti alle organizzazioni governative e alle pubbliche amministrazioni

Il settore pubblico è stato interessato da un importante aumento del numero degli incidenti fra il 2022 e il 2024: questo è spiegabile con l'incremento delle attività dimostrative, di disturbo e di fiancheggiamento legate ai conflitti in corso, le quali hanno come obiettivi di elezione soggetti legati alle sfere governative e della difesa di quei Paesi considerati avversari, e dei loro alleati o amici.

Tra il 2020 e il 2024 il campione ha incluso 1.393 incidenti noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Globalmente la crescita è più che lineare, ed al forte incremento registrato fra il 2022 e il 2023 è seguito un aumento ancora più significativo fra il 2023 e il 2024. Nell'arco dei cinque anni si è comunque passati dai 208 incidenti del 2020 ai 431 del 2024, con un incremento complessivo di oltre il 100% (Fig. 19).

+100%
è la crescita degli incidenti nel settore GOV dal 2020 a oggi

La distribuzione degli attaccanti (Fig. 20) mostra chiaramente l'ulteriore aumento del fenomeno Hacktivism, in crescita sin dal 2022: il numero di incidenti generato da questa categoria di attaccanti è cresciuto di oltre il 50% fra il 2023 e il 2024.

+50%
è la crescita degli incidenti di tipo Hacktivism nel settore GOV nell'ultimo anno

Tecniche di attacco

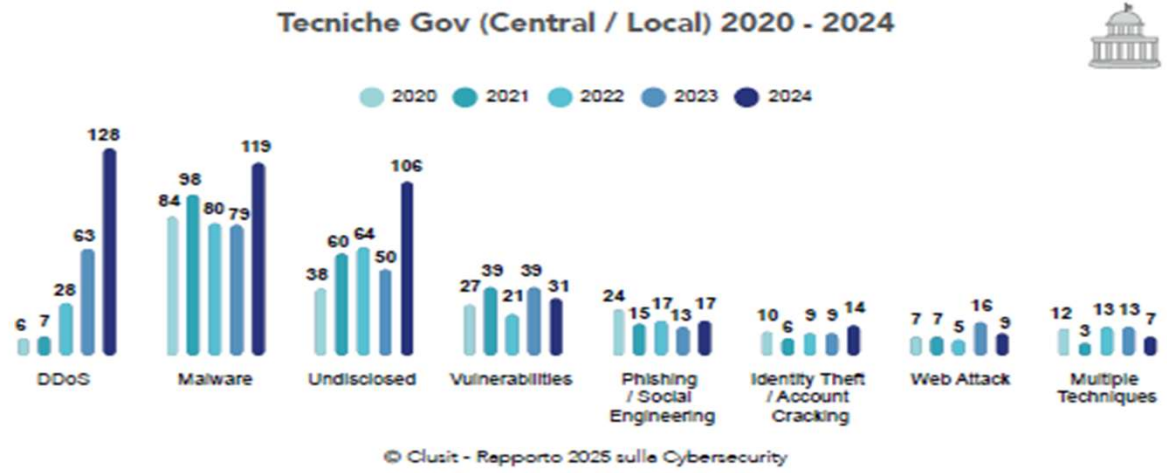

Fig. 22 - Distribuzione delle tecniche di attacco nel settore Gov (Central / Local) nel periodo 2020-24

2x

è la crescita degli incidenti DDOS nel settore GOV nell'ultimo anno

Per quanto riguarda le tecniche utilizzate (Fig. 22) notiamo che gli incidenti causati da *DDoS*, tipici dei fenomeni di attivismo, sono più che raddoppiati anche nell'ultimo anno, così come era già successo nell'anno precedente; quelli mediante *Malware* sono cresciuti del 50%, mentre sono rimasti sostanzialmente costanti tutti gli altri. Cresce molto, tuttavia, la quota di incidenti per cui le tecniche impiegate non sono state rese note, oltre il doppio rispetto all'anno precedente.

Cos’è un incidente informatico

Definizione di incidente nella Direttiva Nis 2

- **Art 6, 6)** «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;

- **Art 23, paragrafo 3**: Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Tipologia di incidenti1/2

Un incidente, che può avere molteplici vettori di attacco, interni ed esterni, può colpire sistemi, dati o servizi; spesso con effetti che si ripercuotono sia sulla sicurezza che sulla privacy:

Se c’è un incidente informatico c’è spesso un Data breach

Tipologie di incidenti 2/2

- Attacchi DDoS: interruzione servizi online pubblici
- Malware e ransomware: blocco servizi, cifratura dati
- Phishing e social engineering: furto credenziali, accessi non autorizzati
- Errori umani e configurazioni errate: dati pubblicati o esposti accidentalmente

- Gli incidenti informatici nella PA possono essere classificati in base all’**IMPATTO**, al tipo di violazione e alla causa.
  La classificazione è essenziale per capire a chi notificare l’evento, con quale priorità e con quali contromisure.
  In pratica, la PA deve essere in grado di dire rapidamente: *Cosa è successo? Quanto è grave? È causato da un attacco o da un errore interno? Coinvolge dati personali?* Solo così potrà rispettare le scadenze della NIS2 e del GDPR.”

Mappatura delle norme

NIS2 (D.Lgs. 138/2024) - Soggetti Essenziali ed Importanti

- La Direttiva NIS2, recepita nell'ordinamento italiano con il D.Lgs. 138 del 2024, amplia e aggiorna il perimetro dei soggetti obbligati ad adottare misure di cybersicurezza rafforzata.
  Essa distingue tra soggetti essenziali e soggetti importanti, imponendo a entrambi stringenti obblighi di gestione del rischio e di notifica degli incidenti significativi.
- Le **Pubbliche Amministrazioni** sono comprese espressamente nell'**Allegato III** del decreto di recepimento: ciò significa che anche gli enti pubblici – non solo centrali ma anche territoriali e locali di una certa dimensione – sono riconosciuti come operatori fondamentali per il buon funzionamento della vita civile ed economica.
- La ratio è evidente: la PA gestisce una mole considerevole di dati sensibili e critici, e assicura la continuità di servizi essenziali come istruzione, sanità, servizi anagrafici, giustizia digitale e fiscalità. Un incidente informatico che ne comprometta la funzionalità non ha quindi solo un impatto tecnico, ma può tradursi in un grave pregiudizio per i diritti fondamentali dei cittadini e per l'equilibrio stesso delle istituzioni democratiche.

Legge n. 90 del 28 giugno 2024

La Legge 90 del 2024 rappresenta il completamento del quadro normativo delineato dal D.Lgs. 138/2024 di recepimento della Direttiva NIS2.
Se il decreto individua i soggetti obbligati alla disciplina in materia di cybersicurezza, includendo le Pubbliche Amministrazioni nell'Allegato III, la Legge 90 interviene per specificare in maniera puntuale le modalità con cui tali enti devono organizzarsi come l'istituzione del Referente per la cybersicurezza.

Gestione interna degli incidenti

Definizione di «Gestione degli incidenti» nella NIS2

- **Art 6, 8)** «gestione degli incidenti»: le azioni e le procedure volte a **prevenire, rilevare, analizzare e contenere** un incidente o a rispondervi e riprendersi da esso

Linee guida per il rafforzamento della resilienza e referente per la cybersicurezza

▪Oggi la gestione degli incidenti informatici nelle Pubbliche Amministrazioni si basa sulle **Linee guida per il rafforzamento della resilienza emanate dall'ACN**.
Queste linee guida, adottate in attuazione della **Legge 90/2024** e del **D.lgs. 138/2024** (attuazione NIS2), introducono un sistema organico di misure di sicurezza che tutte le amministrazioni devono rispettare.
Il modello proposto dall'ACN non si limita a fornire indicazioni generali, ma definisce misure concrete, con requisiti minimi di implementazione ed evidenze documentali che consentono di verificare il reale livello di applicazione.

▪Le misure riguardano diversi ambiti: dal **censimento degli asset** hardware e software, alla **gestione del rischio e delle vulnerabilità**, fino ai **piani di continuità, risposta e ripristino** in caso di incidente.
In questo contesto, un ruolo fondamentale è svolto dal **Referente per la cybersicurezza**, figura prevista dall'art. 8 della Legge 90/2024.
Egli coordina le attività interne, assicura l'attuazione delle misure stabilite dall'ACN e mantiene il raccordo con l'Agenzia e con il **CSIRT Italia** per la notifica degli incidenti significativi, che devono essere comunicati in tempi molto rapidi (24 ore per la prenotifica, 72 ore per la notifica completa).
La gestione degli incidenti diventa così parte di un sistema strutturato di resilienza, capace di rafforzare la sicurezza delle amministrazioni e garantire maggiore continuità ai servizi essenziali.

Gestione esterna degli incidenti: GDPR/NIS2

Direttiva NIS2/ D.lgs. 138/2024

- Il D.lgs. 138/2024 disciplina il processo di notifica con precise tempistiche e modalità operativa:
- **Entro 24 ore** dalla scoperta: **preallarme** con informazioni essenziali e valutazione preliminare.
- **Entro 72 ore**: **notifica formale**, con aggiornamenti sulle informazioni iniziali .
- **Entro 1 mese**: **relazione finale**, che documenta dettagliatamente l'incidente, le misure adottate e, quando rilevante, l'impatto transfrontaliero
- L'ACN può fornire supporto diretto nella gestione delle notifiche e orientare le comunicazioni verso altri soggetti impattati, ma solo dopo aver sentito il CSIRT

È previsto anche un obbligo di notifica volontaria, per casi non obbligatori, per favorire la cultura della sicurezza e il reporting attivo.

GDPR art. 33-34: gestione dei data breach

- Il GDPR distingue due tipi di obbligo:
- **Notifica al Garante Privacy** (art. 33)
  - Tempistica: entro **72 ore** dalla scoperta della violazione;

  Contenuto minimo: natura della violazione, categorie e numero di dati/utenti coinvolti, conseguenze probabili, misure adottate o pianificate;

  Anche il Responsabile del trattamento deve informare tempestivamente il Titolare, senza ritardi ingiustificati.
- **Comunicazione agli interessati** (art. 34)
  - Necessaria quando la violazione è **ad alto rischio** per i diritti e le libertà delle persone fisiche;

  Deve essere chiara e in linguaggio semplice;

  Può essere omessa se sono state adottate misure che rendono i dati illeggibili (es. cifratura).

Formazione necessaria

- Il Vademecum ACN **Buone pratiche di cybersecurity di base per i dipendenti delle PP.AA.** è una guida operativa realizzata dall'Agenzia per la Cybersicurezza Nazionale (ACN) che fornisce indicazioni pratiche per la protezione dei sistemi informativi, dei dati e dei servizi erogati dalla Pubblica Amministrazione, con l'obiettivo di garantire la loro continuità operativa e resilienza.

Conclusioni

La gestione degli incidenti informatici nella Pubblica Amministrazione non è solo una questione tecnica, ma investe direttamente le responsabilità giuridiche e organizzative degli enti. Il legislatore, con la NIS2 e le norme nazionali di recepimento, ha voluto raggiungere un duplice obiettivo: rafforzare la resilienza delle istituzioni e consolidare la fiducia dei cittadini. Una Pubblica Amministrazione che sa gestire un incidente nel rispetto della legge diventa non solo più sicura, ma anche più affidabile e credibile agli occhi della collettività.

GRAZIE PER L'ATTENZIONE!